PROSEGUR RESEARCH

Luces y sombras del metaverso

2022



PROSEGUR

VISIT…

LANZAROTE
Caliente.COM

Oportunidades

Amenazas



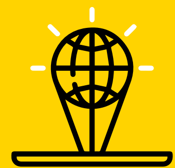


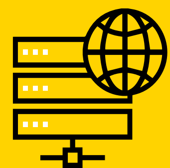
Este documento
es interactivo

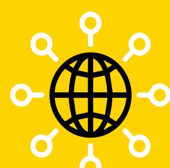


El metaverso es un mundo virtual inmersivo en tres dimensiones con representaciones del entorno y al que se es accesible a través de dispositivos de realidad virtual y aumentada, junto con otras tecnologías como la háptica o los sistemas de reconocimiento que nos permitirán interactuar con todos sus elementos en tiempo real.

El concepto de metaverso no se desarrolla como un videojuego de grandes dimensiones, sino que se cimenta sobre la base de la **socialización virtual:** el objetivo es interactuar con otras personas (**avatares**) mediante espacios públicos, cines, salas de trabajo y zonas de ocio. Así, **las posibilidades son virtualmente ilimitadas**, tantas como en el mundo físico que nos rodea, desde trabajar, cobrar una nómina, asistir a conciertos, visitar museos o hasta estudiar una carrera, por poner solo unos ejemplos.







El metaverso es uno de los **grandes paradigmas de la convergencia tecnológica,** al integrar distintas tecnologías que se apoyan de forma complementaria para ofrecer una experiencia integral al usuario.





Tecnologías vinculadas al metaverso



Realidad virtual

Utilizando dispositivos como las gafas virtuales, se trata de una tecnología que permite la inmersión del individuo en un entorno gráfico generado por ordenador.

Realidad aumentada



Es una tecnología que superpone elementos gráficos a los propios del mundo físico. A modo de ejemplo, destacan las retransmisiones en directo de La Liga de Fútbol Profesional. Junto a la realidad virtual, la realidad mixta o híbrida es la que alcanza la inmersión total del usuario en la visión alternativa.



Tecnología háptica y biométrica

Mediante instrumentos como guantes, gafas y trajes, estas tecnologías se utilizarían con el objetivo de que la interacción y el reconocimiento del avatar se base en el movimiento e información biológica del propio cuerpo humano.

IoT (*Internet of Things*)

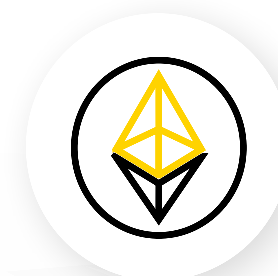


El nivel de interacción entre los entornos físico y digital en el metaverso se verá intensificado por el IoT, gracias a las nuevas oportunidades de interconexión entre diferentes dispositivos.

Computación cuántica



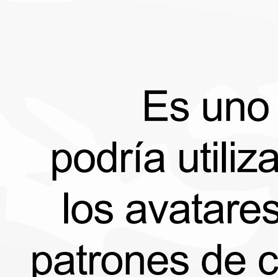
Tipo de computación que permite una variedad de algoritmos exponencialmente superior, lo que incrementa la capacidad de cálculo hasta límites considerados actualmente inalcanzables por ordenadores convencionales.



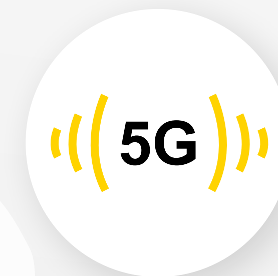
Blockchain

La tecnología *blockchain*, en la que se basan las criptodivisas y los NFT *(Non-fungible tokens)*, podría proporcionar al metaverso una aproximación al concepto de economía y propiedad privada. Los NFT, que se caracterizan por ser únicos, indivisibles y privados, jugarían un importante valor por su capacidad de verificación basada en la cadena de bloques.

Inteligencia artificial



Es uno de los pilares del desarrollo del metaverso, que podría utilizarse como método de análisis de la conducta de los avatares (como movimientos o mensajes) para predecir patrones de comportamiento o hacer más preciso el entorno.



Nuevas generaciones de conectividad móvil (5G, 6G...)

Debido a la mayor velocidad de conexión y la menor latencia de respuesta, se espera que el metaverso potenciado por estas tecnologías sea capaz de ofrecer mejores experiencias al usuario (por ejemplo, mejores gráficos y frames por segundo que con los actuales sistemas de realidad virtual y aumentada).



El metaverso **no es un nuevo concepto** en el imaginario colectivo. Tanto es así que hace ya 30 años, en 1992, el autor Neal Stephenson acuñó el término en su obra *Snow Crash*, donde los personajes interactuaban entre sí en un mundo virtual en 3D. Y este no ha sido el único precedente del metaverso: por ejemplo, un año después, en 1993, Steve Jackson Games lanzó al mercado un sistema de realidad virtual que permitía la conexión simultánea de diferentes usuarios a la vez. **En los últimos años hemos visto aproximaciones de extensos mundos virtuales en la industria del entretenimiento,** destacando los videojuegos de tipo MMORPG como World of Warcraft o sandbox como Minecraft, además de Pokémon GO, primer videojuego de éxito mundial basado en la realidad aumentada y que ha conseguido más de 630 millones de descargas y más de 5.000 millones de dólares en facturación desde su lanzamiento en 2016.

Debemos entender el metaverso como una idea de futuro amplia, no restrictiva y no dominada por una sola compañía. Si bien Facebook parece ser la corporación más pujante sobre el futuro del metaverso con su anuncio de Meta, existen otras empresas, como XRSPACE con su Mova, Microsoft, Apple, Nvidia, Epic Games o Roblox, entre otras, que también se han mostrado interesadas. De hecho, Epic Games ha conseguido expandir las fronteras y posibilidades de su popular videojuego Fortnite, llegando a ofrecer conciertos virtuales en tiempo real, como el de Ariana Grande o Travis Scott, que consiguieron reunir a más de diez millones de jugadores conectados. Otras como Coca-Cola han lanzado su propia colección de NFTs en la plataforma de realidad virtual Decentraland, que cuenta con recursos como las discotecas virtuales personalizadas o la posibilidad de comunicación y entendimiento entre todos los avatares del mundo.

> Todo ello es una muestra de que paulatinamente se está modificando nuestra manera de relacionarnos con la realidad.





El hecho de que exista más de una compañía interesada en la creación de un metaverso pone en duda si se logrará el **principio de interoperabilidad total:** la posibilidad de fluir de código en código y de compartir datos, posibilitando el intercambio de información entre diferentes sistemas. A día de hoy, el metaverso tal y como se plantea se acerca más a un propósito que a una realidad: los expertos señalan las grandes **barreras** que frenan su desarrollo como los **dispositivos tecnológicos** de realidad virtual suficientemente precisos o el **diseño**, en términos de la **infraestructura necesaria** con la que tendría que contar este universo alternativo (desde rascacielos hasta calles, supermercados y semáforos). Así, la capacidad de interoperabilidad parece algo utópico: ¿cómo se podría lograr la conexión entre dos usuarios que utilicen distintos "metaversos empresariales"? ¿Estarían dispuestas las empresas a compartir información de los usuarios en aras de lograr una auténtica conexión entre estos mundos virtuales?

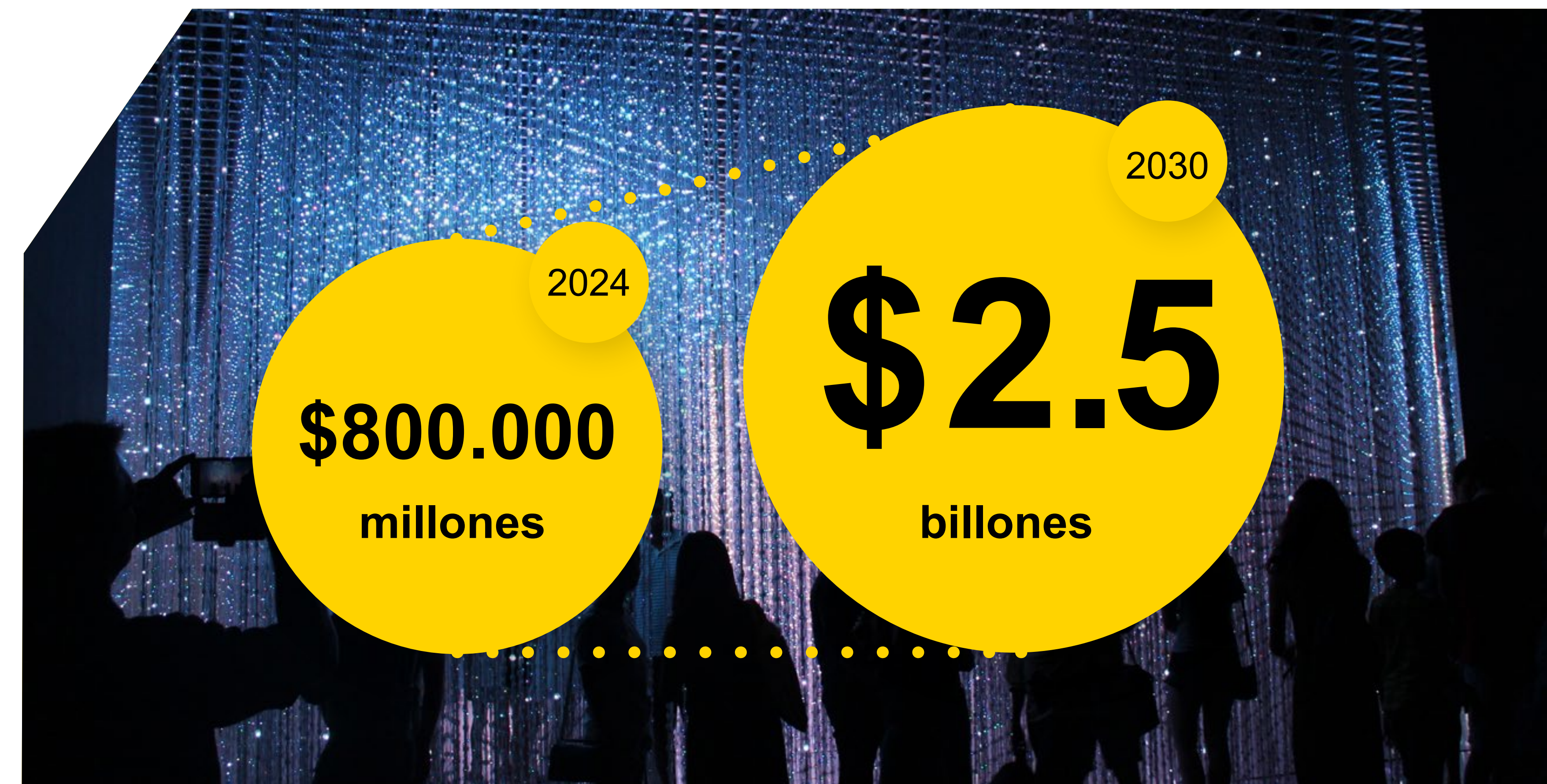
La potencialidad económica del metaverso parece que no tiene freno. Ya en 2021 los últimos datos de Bloomberg Intelligence situaban el valor del metaverso en 500 000 millones de dólares. Pero eso no es todo: también apuntan que su oportunidad de mercado oscilará en aproximadamente **800 000 millones de dólares para 2024 y en 2.5 billones de dólares para 2030[1].** Además, Bank of America ha señalado el metaverso como una de las catorce disrupciones tecnológicas que podrían transformar nuestras vidas.

[1] De manera paralela, Grayscale cifraba los ingresos de los mundos virtuales de los videojuegos en 180 000 millones de dólares en 2020, lo que podría aumentar hasta los 400 000 millones para 2025.

Estas optimistas expectativas económicas se deben a sus infinitas posibilidades, como ya hemos mencionado brevemente, y a su capacidad de darle un giro al **panorama laboral y del desarrollo de los videojuegos, la programación y las redes sociales[2].** De hecho, la Estrategia Nacional de Largo Plazo España 2050 señala el crecimiento del metaverso y de la realidad virtual como uno de los vectores del desarrollo tecnológico, con la consecuente creación de empleo, como los data scientists, operadores de robots o los más controvertidos jardineros de Minecraft y entrenadores de avatares.

Sin embargo, el metaverso también plantea una serie de **desafíos para la seguridad** que empresas y usuarios debemos tener en cuenta.

[2] Por ejemplo, Meta ya ha anunciado su plan de contratación de 10 000 personas de la Unión Europea en los próximos años dedicadas exclusivamente al desarrollo del metaverso





Desafíos para la seguridad

Los avances en el desarrollo del metaverso implican la aparición de nuevos riesgos y desafíos, obligando a los garantes de la seguridad a anticiparse a la imaginación y la falta de límites o condicionantes éticos y legales de quienes emplean los avances de forma maliciosa.

A este respecto, la **hiperindividualización de los contenidos y servicios,** la explotación económica del metaverso, el anonimato y el traslado de las problemáticas sociales comunes al ciberespacio como la discriminación de todo tipo o la polarización social favorecen el auge de conductas delictivas.

A continuación, se señalan algunos de los potenciales usos delictivos o aplicaciones maliciosas que pueden aprovechar el desarrollo del metaverso y de sus tecnologías asociadas para expandirse.

Traslado de la conducta social al metaverso

Como ha ocurrido tanto con Internet como con el denominado “metaverso primitivo” de ***Second Life,*** es probable que gran parte de la actividad desarrollada en futuros metaversos se oriente al consumo de contenido para adultos, por lo que esta circunstancia presenta importantes retos en materia de protección de personas como veremos a continuación.





Conducta violenta

El traslado de la interacción social al plano virtual implica, el traslado de las conductas violentas de acoso, abuso y coerción. En este sentido, es probable que las interacciones entre los avatares lleven a la ocurrencia de un número cada vez mayor de situaciones que tengan un impacto tangible en la realidad, de manera similar a como ocurre con el acoso o la coerción en redes sociales, y que estas se desarrollen en una esfera de impunidad, aprovechando que la lentitud con la que el **ordenamiento jurídico** se adapta a la innovación en la conducta criminal.

Captación y radicalización



La enorme oferta digital, así como la ausencia de registro de las comunicaciones, (tanto de viva voz como mediante el aprovechamiento de los espacios físicos de los juegos, como la escritura de mensajes con el trazado de los pasos o las armas), y la sensación de anonimato que subyace a la mayoría de plataformas de juego, facilita enormemente que puedan desarrollarse “interacciones sensibles” para captar a jóvenes en las filas de organizaciones criminales o terroristas. Además, la inmersión en el metaverso favorece la desensibilización sistemática del usuario implicado en el proceso de radicalización, mediante su exposición en realidad virtual a contenidos de carácter violento.



Extorsión

El empleo de avatares por parte de delincuentes -mediante la grabación de conversaciones o interacciones- permite extorsionar a los consumidores de contenidos amenazándoles con publicar información personal.

Exposición de menores



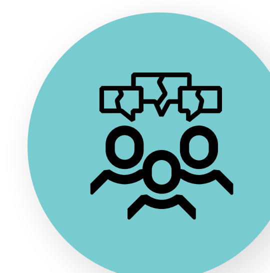
Pese a que la expresión virtual del usuario (el avatar) carece de presencia física como tal, el hecho de que las interacciones entre usuarios sean reales y puedan desarrollarse sin supervisión potencia la probabilidad de que circunstancias como el anonimato permite que menores con curiosidad se expongan a todos los riesgos mencionados.



Suplantación de identidad

Las personas podrían ser víctimas de robo de datos, ya sean personales o biométricos, que posteriormente pueden ser comercializados o utilizados de manera ilícita, ya sea en el propio metaverso o en el mundo físico. Es por ello que la suplantación de la identidad, también conocido como *spoofing,* es uno de los temas que más preocupan en el desarrollo de este nuevo universo digital.

Polarización social



Lo cierto es que existe un alto riesgo de polarización política y social en el metaverso que podría suponer su desarrollo. La combinación de las tecnologías de realidad aumentada, realidad virtual e inteligencia artificial podrían suponer una visión del mundo característica y única para cada usuario, por lo que se ha señalado que se podría llegar a bloquear visual y/o auditivamente contenido que no esté acorde a los gustos o ideas de cada persona. Además, y unido a la utilización de la información biométrica recabada, se ha especulado sobre la posibilidad de incluir publicidad individualizada, lo que abriría las puertas a la monetización del metaverso.



Aparición de un nuevo espacio para la delincuencia económica

Veremos posibilidades de explotación económica en el metaverso nunca imaginadas hasta ahora; aunque esto sea un aspecto negativo, implica ciertos riesgos. El rápido flujo de transacciones y el hecho de que **ni el metaverso ni los espacios económicos cripto estén suficientemente regulados todavía** ha provocado que este escenario se configure como un elemento atractivo para estafadores y ciberdelincuentes.

En este nuevo entorno, el desconocimiento del sistema de transacciones del metaverso por parte de usuarios y empresas puede facilitar el éxito de estafas mediante, por ejemplo, **contratos inteligentes** que no hacen lo que aparentemente prometen, sino que ofrecen acceso a los criptoactivos o la información personal de la víctima.

También han de señalarse los riesgos típicos que encontramos actualmente en Internet y que no parece que vayan a estar exentos en el metaverso. Por ejemplo, los **ataques de denegación de servicio distribuido (DDoS),** los cuales tratan de colapsar servidores al recibir más peticiones de las que pueden soportar, podrían utilizarse contra los servidores del propio metaverso, a fin de interrumpir su funcionamiento. Además, la economía basada en criptomonedas, apoyada por la tecnología *blockchain* y los NFT, podría suponer la compraventa de activos digitales preciados, tales como obras de arte o terrenos digitales, lo que será un objetivo para los ataques ***ransomware,*** que tratan de secuestrar los datos almacenados solicitando un rescate económico para poder descifrar dicha información.



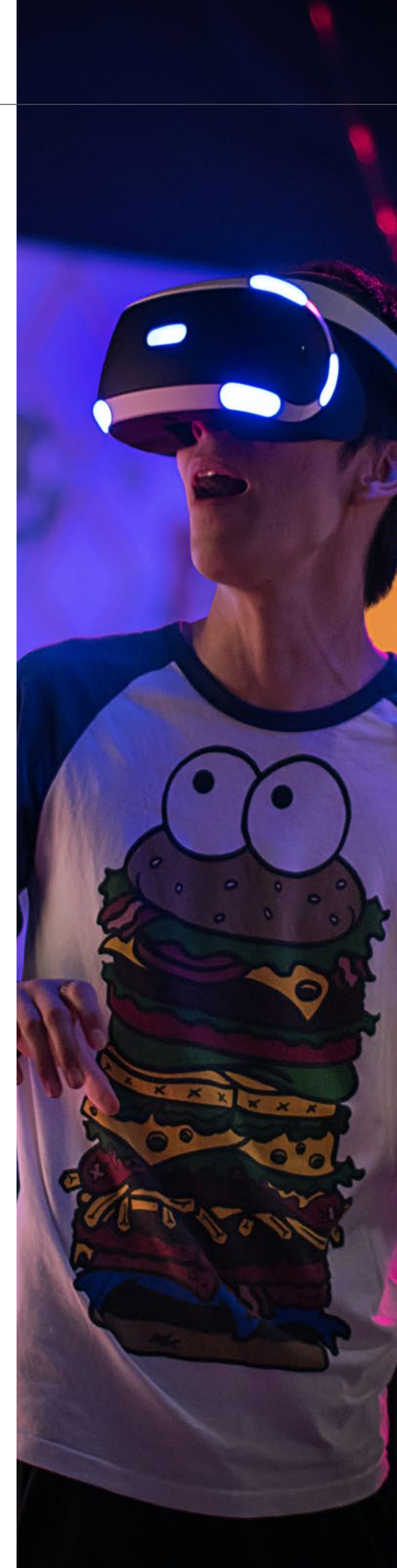
Gamificación perversa

La utilización de dispositivos de realidad aumentada de manera imprudente o descuidada puede implicar serios desafíos para la seguridad al **asumir conductas de riesgo o al situar a personas sin intención criminal en situaciones comprometidas.** A este respecto, destaca el gran número de casos de violaciones de perímetros y áreas de acceso restringido acaecidas a nivel global por causa del fenómeno Pokémon GO. Esta situación ha llevado al Cuerpo de Marines de los Estados Unidos a realizar **una publicación con recomendaciones** para que los jugadores eviten acceder a zonas restringidas mientras juegan.

Asimismo, la inmersión de los usuarios en el metaverso incrementa la probabilidad de que se produzcan situaciones de **disociación de la realidad,** mediante la participación de estos en juegos perversos, como ocurrió recientemente con el caso de la **Ballena Azul,** un desafío de terror que acababa con la inducción al suicidio de sus participantes. En este sentido, los elementos de realidad virtual y realidad aumentada facilitan que este tipo de **esquemas de coerción y manipulación** tengan un mayor impacto sobre las víctimas, permitiendo su captación e implicando un riesgo físico real y tangible para su integridad física.

Además, **la gamificación en un contexto inmersivo facilita herramientas de una inédita potencia a la hora de llevar a cabo acciones de manipulación,** dado que altera el vector de influencia sobre las víctimas, pasando de ser externo (se convence a la víctima) a interno (el propio progreso). En este escenario, es probable que el desarrollo de estas tecnologías lleve a la aparición de espacios y grupos dedicados a extraer beneficios derivados de la manipulación de los usuarios en el metaverso, configurándose como sectas o clanes que lleven a cabo una explotación económica.

Asimismo, no podemos obviar los **riesgos físicos para el usuario,** como los mareos, las caídas o las "ciber-enfermedades", según apunta el Foro Económico Mundial (WEF) al señalar efectos a largo plazo tales como la pérdida de coordinación visual.



En foco. Milsim y filtraciones de defensa en el metaverso

El desarrollo de motores gráficos y lógicos cada vez más potentes (derivados de la evolución de la capacidad computacional) permite **aproximaciones digitales cada vez más realistas,** siendo frecuente que los entornos de simulación repliquen escenarios, físicas, materiales, procedimientos y acciones muy similares a la realidad. No en vano, ejércitos profesionales de países como EE. UU. ya emplean sistemas de simulación militar (Milsim) y dispositivos de realidad virtual para llevar a cabo entrenamientos.

En este contexto, destaca el género de videojuegos Milsim (simulación militar) como un **potencial foco de filtraciones de información de defensa** que pueden suponer un riesgo para la seguridad. Esto se debe a la confluencia entre la percepción de bajo riesgo que suscitan los entornos de juego y la habitualmente elevada presencia de personal militar con acceso a conocimientos de carácter restringido. El esfuerzo por representar fielmente infraestructuras militares, equipo, armamento, tácticas o procedimientos, pese a no implicar mala intención, se configura como un riesgo potencial de que dichos conocimientos acaben en manos de delincuentes o actores terroristas.



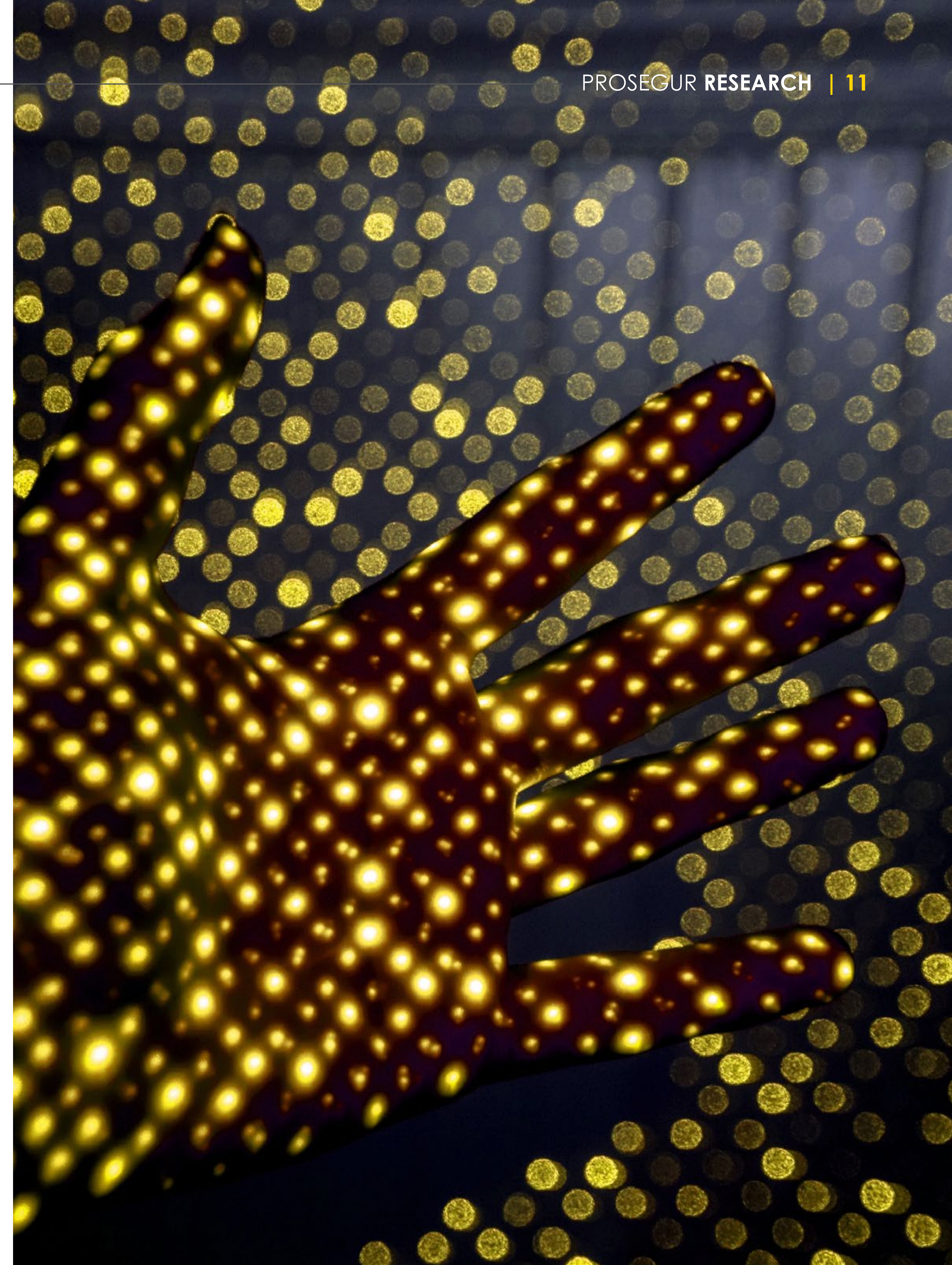
El metaverso como e-learning criminal

En un contexto en el que las comunicaciones convencionales son fácilmente rastreables por parte de las autoridades responsables de controlar la amenaza terrorista, **el metaverso se configura como un escenario ideal para el aumento de las actividades de transmisión de conocimientos y planificación de operaciones para los organizaciones criminales y terroristas.** Esto se debe a los siguientes factores:

- Los metaversos basados en el principio Sandbox permitirían **replicar escenarios de futuros atentados** con relativa exactitud, mejorando la planificación y el desempeño futuro de los activos terroristas. A modo de ejemplo de la planificación en Sandbox, se señala que tres de los terroristas del 11-S, se entrenaron para volar aviones grandes en un simulador de vuelo, que probablemente contaba con una potencia gráfica muy inferior a la de cualquier simulador de aviación civil convencional actual.

- Es muy probable que el **desarrollo progresivo de la Inteligencia Artificial** aplicada a los NPCs *(Non-Playable Characters)* permita simular una respuesta cada vez más real por parte de las fuerzas de seguridad, los servicios de emergencias o los civiles, contribuyendo también a la calidad de los entrenamientos de activos en el metaverso.

Este servicio de e-learning criminal es extensible a cualquier grupo o particular con interés de aprender y con propósito de delinquir; y facilitará más que nunca la comunicación, el aprendizaje y el desarrollo de estrategias, configurándose como un desafío para las fuerzas de seguridad.





A todas estas amenazas debe añadirse el **gran desafío legal** que supone el metaverso.

La descentralización de internet y la carencia de adaptaciones del ordenamiento jurídico a esta nueva realidad limita en gran medida las posibilidades de regulación específica de muchos comportamientos delictivos de los usuarios, así como la judicialización y prevención de los mismos. Además, la protección de la privacidad y la propiedad intelectual son dos aspectos importantes planteados a raíz del desarrollo teórico y práctico del metaverso.

La tecnología es un medio y el metaverso se postula como un **motor de cambio,** innovación y convergencia. Por ello, no debemos olvidar que el **factor humano** es el que realmente genera los riesgos y también quien tiene la posibilidad de anticiparlos y construir un entorno seguro, a la altura del desarrollo tecnológico en el que nos encontramos.

> En definitiva, nos encontramos ante un futuro apasionante, si bien no exento de importantes desafíos, sobre el que construir todo un entorno interactivo multidimensional y con un gran potencial transformador.



Garantizamos la seguridad de las personas, las empresas y la sociedad en su conjunto.